State of Vermont

System/Service Password Policy

VERMONT

Contents

1.0 Introduction

1.1 Authority

VSA 22 § 901 (1), authorizes the Department of Information and Innovation "to provide direction and oversight for all activities directly related to information technology and security in state government."

1.2 Purpose

Passwords are an important component of information technology and network security. The use of a password in combination with the user name serves to identify those who are authorized to have access to system resources and information assets. Authenticated access is one way that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used, changed on a regular basis and protected appropriately to ensure that the level of security they imply is actually met.

The purpose of this policy is to provide the guidelines necessary for IT professionals of the State of Vermont as well as IT professionals who are state partners, vendors, contractors with accounts, to create appropriate system passwords and to use them and protect them in an appropriate manner.

1.3 Scope

This is one of two policies that address passwords.

The scope of this policy applies to passwords used by State of Vermont devices (system or service accounts), networks and other systems (i.e. servers, switches, routers etc.).

This policy will address accounts and passwords used by IT professionals for the administration of systems.

2.0 Policy

Passwords are the foundation of virtually all access and user management security systems. Passwords typically allow access to the data managed and controlled by departments and agencies. The complexity, use, and management of passwords should reflect the classification of the data that is being protected or accessed. There may be instances where two-factor authentication or biometrics may be required to access specific accounts. If that is the case, this should be reflected in a specific agency or department written procedure.

2.1 General

Accounts used to run system services, unlike user specific accounts, may not always be able to have password changes implemented at specific intervals due to possible disruption of process or maintenance schedules.

2.2 Password Implementation

System passwords will comply with the guidelines within this policy unless a waiver is submitted. (See section 4.0 concerning waivers.)

1. Service account passwords will be changed a minimum of every sixty (60) days.
2. Service account passwords shall be a minimum length of eight (8) characters in a combination of upper and lower case alpha, numeric, and special characters.
3. Default vendor passwords shall be changed during or immediately after installation of the information system product.
4. Password changes shall be systematically enforced where possible.
5. Accounts shall be systematically disabled after ninety (90) days of inactivity to reduce the risk of compromise.

3.0 System Password Protection

There are general guidelines that have to be adhered to for passwords to be effective. These guidelines are listed below.

1. Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at a system password to any unauthorized person(s). Since systems are managed by more than one person, passwords shall be administered on a need-to-know basis only. If system passwords are "predetermined or sequential" they are to be kept locked in a secure area at all times.
2. Passwords shall not be transmitted electronically over the unprotected Internet, such as via e-mail.
3. No employee is to keep an unsecured written record of passwords, either on paper or in an electronic file unless kept in a controlled access safe or an encrypted file.
4. If an employee either knows or suspects that a system password has been compromised, it must be changed immediately and reported to the IT department manager.
5. If an employee terminates employment, it is necessary to change system passwords that the employee has knowledge of. Each agency/department is responsible for documenting these requirements within their written procedure.

3.1 Training

Each State agency is responsible for ensuring that its employees are properly trained in accordance with this policy and any related internal agency policies and procedures. The Department of Information and Innovation will work with Agencies and The Summit: Center for State Employee Development to identify appropriate training opportunities.

3.2 Enforcement

Any employee found to have violated this policy may be subject to loss of privileges and/or disciplinary action, up to and including termination of employment.

4.0 Waiver

There may be instances when this policy can not be followed due to system functionality, maintenance requirements, or other reasons. Because of this fact, an agency/department may request a waiver. The waiver will be submitted stating the reason for the waiver, what part of the system password policy requires an exception and how the issue will be addressed.

See Appendix A for **System/Service Password Waiver** form.

1. Waivers must be submitted to the Office of the Security Director and a copy kept within the department or agency for reference, such as a security audit.
2. The waiver must be signed by the appropriate IT department stewards responsible for the particular system.

Issuing Entity: Office of the Secretary, Agency of Administration

Approved: _____ Date: ___2/15/10___

Secretary of Administration

Appendix A:

Service Password Waiver Form to be filled out and returned to the Office of the Security Director.

Service Password Waiver	
Agency/Department Requesting waiver	
Service/System	
Reason for exception:	
Submitted by: Title:	
Date Submitted:	
Reviewed by: Title:	
Date Approved:	